AMENDMENT TO THE CLAIMS

Amendments to the claims are reflected in the following listing, which replaces any and all prior versions and listings of claims in the present application:

LISTING OF CLAIMS:

Claims 1-4 (canceled).

Claim 5 (Currently Amended) A method for protecting a network server from being used as the basis of an attack on a network client, the method comprising:

~~a. restricting access to said network server to a trusted portion of said network server for at least a selected protocol;~~

~~b.~~ scanning ~~said~~ a trusted portion of said network server ~~for~~ to find executable commands inserted by an unwanted party, said executable commands being associated with ~~said~~ a selected ~~protocol~~ programming language, wherein said trusted portion is a subset of said network server; and,

~~c.~~ editing ~~each of~~ at least a portion of said executable commands such that said executable commands still remain in said trusted portion, but ~~will~~ cannot be executed by ~~the~~ said network client ~~server~~.

Claim 6 (canceled)

Claim 7 (Currently Amended) The method of Claim 5, ~~further comprising~~ wherein said editing of said executable commands comprises replacing particular characters within said executable commands.

Claim 8 (Currently Amended) The method of Claim 5, further comprising rejecting a request when said request contains said executable commands having a hostile character. ~~wherein said executable commands include particular characters and said characters are hostile characters and wherein if a request contains any of said hostile characters, the request is rejected.~~

Claim 9 (Previously Presented) The method of Claim 5, further comprising logging said executable commands to form a security log.

Claim 10 (Previously Presented) The method of Claim 9, further comprising reviewing said security log to determine whether said executable commands are hostile.

Claim 11 (Currently Amended) The method of Claim 5, wherein said ~~protection of the network server~~ scanning is accomplished during an electronic purchase transaction.

Claim 12 (Currently Amended) The method of Claim 11, wherein ~~the~~ said electronic purchase transaction is conducted using a digital wallet.

Claims 13-50 (Canceled).

Claim 51 (New) The method of Claim 5, wherein said executable commands cause an unwanted action when executed.

Claim 52 (New) The method of Claim 5, wherein said executable commands are malicious.

Claim 53 (New) The method of Claim 5, further comprising receiving a request for a connection at said network server from said network client.

Claim 54 (New) The method of Claim 53, further comprising verifying that a response from said network server to said network client is void of said executable commands.

Claim 55 (New) The method of Claim 54, further comprising providing said response from said network server to said network client.

Claim 56 (New) The method of Claim 5 wherein said programming language comprises javascript.

Claim 57 (New) A method for prevention of a network attack comprising:

sending, from a network client, a request for a connection to a network server, wherein said network server scans a trusted portion of said network server to find an executable command inserted by an unwanted party into said request, said executable command being associated with a selected programming language, wherein said trusted portion is a subset of said network server; and, said network server edits at least a portion of said executable command for insertion into a response, such that said executable command still remains in said trusted portion, but cannot be executed by said network client; and,

receiving, by said network client, said response from said network server.